ON MODULAR FORMS AND ELLIPTIC CURVES OVER $\mathbb{Q}(\zeta_5)$ (Automorphic forms, trace formulas and zeta functions)

AUTHOR(S):

YASAKI, DAN

数理解析研究所講究録
第1767巻 2011年 133-145

ON MODULAR FORMS AND ELLIPTIC CURVES OVER $\mathbb{Q}(\zeta_5)$

DAN YASAKI

ABSTRACT. We survey our joint work with Paul Gunnells and Farshid Hajir on a computational investigation of the modularity of elliptic curves over the cyclotomic field $\mathbb{Q}(\zeta_5)$, including the techniques we developed for describing the action of the Hecke operators using Voronoï theory.

1. INTRODUCTION

Let E be an elliptic curve over $\mathbb{Q}$. Work of Wiles et al. [BCDT01, CDT99, Dia96, Wil95, TW95] shows that E is modular, i.e. there exists a holomorphic modular form f of weight 2 with integer Fourier coefficients such that

$$L(s, E) = L(s, f).$$

Conversely, starting with a classical newform of weight 2 with integer Fourier coefficients, the Eichler-Shimura construction gives a way to construct an elliptic curve with matching L-function.

The Langlands program predicts that such correspondences should be true for arbitrary number fields. In joint work with P. Gunnells and F. Hajir [GHY11], we investigate the analogous problem over a cyclotomic field. Specifically, let ζ_5 be a primitive fifth root of unity and let $F = \mathbb{Q}(\zeta_5)$. We investigate modularity of elliptic curves over F. By modularity, we mean that for an elliptic curve E over F of conductor $\mathfrak{n}$, there should exist an automorphic form f on GL_2, also of conductor $\mathfrak{n}$, such that we have equality of partial L-functions

$$L_S(s, f) = L_S(s, E),$$

where S is a finite set of places including those dividing $\mathfrak{n}$. Conversely for an appropriate automorphic form f, there should exist an elliptic curve E/F.

More precisely, we investigate the group cohomology for the linear algebraic group $\mathbf{G} = \mathrm{Res}_{F/\mathbb{Q}}\,\mathrm{GL}_2$ and $\Gamma = \Gamma_0(\mathfrak{n})$ the congruence subgroup of $\mathrm{GL}_2(\mathcal{O})$ with bottom row congruent to $(0, *) \mod \mathfrak{n}$. Our work focuses on a particular cohomology space attached to Γ, namely $H^5(\Gamma; \mathbb{C})$. We compute the dimension of this cohomology space for a range of levels and compute the action of the Hecke operators.

These cohomology classes represent concrete realizations of certain automorphic forms. One can exploit this link between automorphic forms and cohomology classes by using topological methods. The purpose of this note is to give an introduction to the techniques, developed in [GHY11, GY08, Yas09a] that we used to perform these computations.

The Voronoï polyhedron is a space with natural tessellation by polytopal cones on which $\mathrm{GL}_2(\mathcal{O})$ acts. Certain automorphic forms, and the Hecke action on these forms can be described in terms of the cones. In Section 2, we present the classical case of holomorphic modular forms for $\mathrm{SL}_2(\mathbb{Z})$ in this language. These concepts are generalized in Section 3, where the *sharblies* are used in place of modular symbols. Finally, we discuss our computational results Section 4, which indicate relationships between $H^5(\Gamma; \mathbb{C})$ and elliptic modular forms, Hilbert modular forms, and abelian varieties.

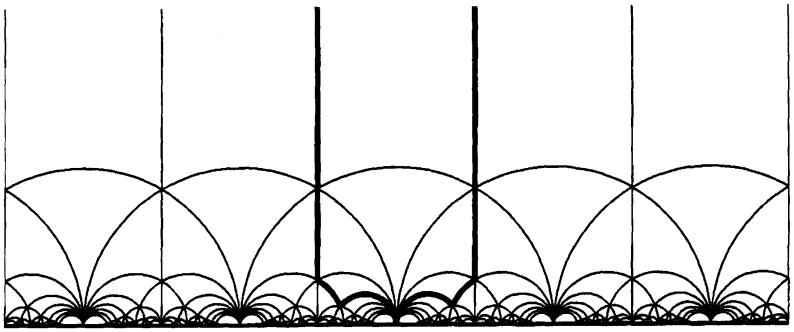


FIGURE 1. A fundamental domain for $\Gamma_0(5)$.

Acknowledgments. This article is based on a lecture delivered by the author at the 2011 RIMS conference *Automorphic forms, trace formulas, and zeta functions.* The author thanks the organizers of the conference, Yasuro Gon (Kyushu University) and Tomonori Moriyama (Osaka University), for the opportunity to speak. He also warmly thanks Takayuki Oda and Takahiro Hayata for the invitation to Japan and for being such excellent hosts. Finally, he thanks Paul Gunnells and Farshid Hajir for working with me on such a fun project.

2. MOTIVATING EXAMPLE

In this section we present part of the theory of holomorphic weight 2 modular forms of level N in the context of Voronoï theory. We relate the modular symbol algorithm to a geometric process in a cone of positive definite quadratic forms. These ideas will be generalized in Section 3.

2.1. **Background.** Let $\mathfrak{h}$ be the complex upper half-plane. The group $G = \mathrm{SL}_2(\mathbb{R})$ acts transitively on $\mathfrak{h}$ by fractional linear transformations

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \frac{az+b}{cz+d}.$$

The stabilizer of $i \in \mathfrak{h}$ is $K = \mathrm{SO}(2)$, and hence we can identify the upper half-plane with the coset space $\mathfrak{h} \simeq G/K$.

Let

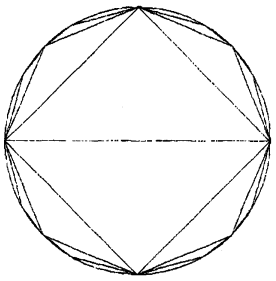
$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \bmod (n) \right\}.$$

Note that $\Gamma_0(N)$ acts on $\mathfrak{h}$ as above, and we can consider the quotient space under this action. Since $\Gamma_0(N)$ has finite index in $\mathrm{SL}_2(\mathbb{Z})$, a fundamental domain for $\Gamma_0(N)$ consists of finitely many translates of a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$. A fundamental domain for $\Gamma_0(5)$ is shown outlined in a dark line in Figure 1.

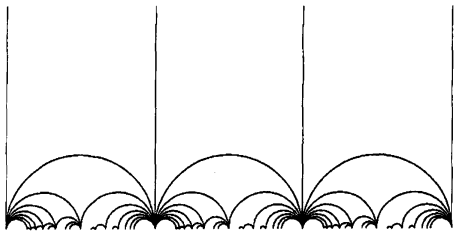
The Eichler-Shimura isomorphism [Hab83]gives that

$$H^1(\Gamma_0(N); \mathbb{C}) \simeq S_2(N) \oplus \overline{S_2(N)} \oplus \mathrm{Eis}_2(N),$$

where $S_2(N)$ is the space of cusp forms and $\mathrm{Eis}_2(N)$ is the space of Eisenstein series of weight 2 and level N. The group cohomology $H^*(\Gamma_0(N); \mathbb{C})$ is isomorphic to the cohomology $H^*(\Gamma_0(N)\backslash\mathfrak{h}; \mathbb{C})$. Each of these maps is an isomorphism of Hecke modules.



Tessellation of C into polytopal cones.



Tessellation of $\mathfrak{h}$ by ideal triangles.

FIGURE 2. Tessellations coming from Voronoï polyhedron.

2.2. **Positive definite forms.** Let V denote the 3-dimensional real vector space of 2×2 symmetric matrices. Every binary quadratic form

$$\phi(x, y) = ax^2 + bxy + cy^2, \quad \text{where } a, b, c \in \mathbb{R},$$

can be represented by a symmetric 2×2 matrix

$$A_\phi = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}.$$

In this way, we identify V with the space of binary quadratic forms. Let $C \subset V$ be the 3-dimensional open cone of positive definite quadratic forms. This is the cone defined by $b^2 - 4ac < 0$ with $a > 0$.

Define a map $q\colon \mathbb{Z}^2 \to \bar{C}$ by

$$q(v) = vv^t.$$

Note that $q(v)$ is a rank 1 quadratic form on the boundary $\bar{C} \setminus C$ of C.

There is an inner product $\langle \cdot, \cdot \rangle$ on V which respects the interpretation of V as a space of quadratic forms. For symmetric matrices $A, B \in V$, we define

$$\langle A, B \rangle = \mathrm{Tr}(AB).$$

Note that for $v \in \mathbb{Z}^2$, we have

$$\langle \phi, q(v) \rangle = \mathrm{Tr}(A_\phi vv^t) = \mathrm{Tr}(v^t A_\phi v) = \phi(v).$$

In this way, we can view the evaluation of quadratic forms at integer vectors as the inner product between certain vectors in V.

We are now ready to construct the Voronoï polyhedron associated to $\mathrm{SL}_2(\mathbb{Z})$. This polyhedron, and generalizations for $\mathrm{SL}_n(\mathbb{Z})$, were introduced by Voronoï in his study of positive definite quadratic forms [Vor08].

Definition 2.1. The *Voronoï polyhedron* Π is the closed convex hull in $\bar{C}$ of

$$\{q(v) \mid v \in \mathbb{Z}^2 \setminus 0\}.$$

The boundary of the Voronoï polyhedron consists of infinitely many triangular facets with vertices (necessarily) at the boundary of C. By taking cones over these faces, we get a decomposition of C into polytopal cones. This decomposition of C scaled onto the trace 1 slice of C is shown in Figure 2.

Note that $G = \mathrm{SL}_2(\mathbb{R})$ acts transitively on $\mathfrak{h}$, and the stabilizer of $i \in \mathfrak{h}$ is $K = \mathrm{SO}(2)$. It follows that we have the identification $\mathfrak{h} \simeq G/K$. Furthermore, G acts transitively on

the determinant 1 sheet of matrices in C, and the stabilizer of I is SO(2). Thus we can identify the cone modulo homotheties with G/K. We have

$$\mathfrak{h} \simeq G/K \simeq C/\mathbb{R}_{>0}$$
$$g \cdot i \mapsto gK \mapsto \mathbb{R}_{>0} \cdot gg^t.$$

Under this identification, the cusps $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ of $\mathfrak{h}$ correspond to the vertices of Π. Furthermore, $\mathrm{SL}_2(\mathbb{Z})$ acts compatibly on each space (also on the cusps).

2.3. **Modular symbols.** One wishes to understand the action of Hecke operators on spaces of cusp forms. This action can be computed in terms of modular symbols, developed since the 1960s by Birch, Manin, Shokorov, Mazur, Merel, Cremona, and others.

Modular symbols are a formal sum symbols $\{\alpha, \beta\}$, where $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ modulo the relations

1. $\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} = 0$,
2. $\{\alpha, \beta\} = -\{\beta, \alpha\}$,
3. $g \cdot \{\alpha, \beta\} = \{\alpha, \beta\}$ for all $g \in \Gamma_0(N)$.

We identify each cusp $\alpha = a/b$ with the vector $(a, b)^t$, with the convention that ∞ corresponds to the vector $(1, 0)^t$. Then we call a symbol unimodular if the determinant of the 2×2 matrix created with the associated vectors is ± 1.

Unimodular symbols form a finite generating set for the modular symbols, and so for computer calculations, one often wishes to express everything in terms of unimodular symbols. The action of Hecke operators sends a unimodular representative to a non-unimodular one, and so we must use the relations to re-express the non-unimodular symbol as a sum of unimodular symbols. The usual technique for this involves continued fractions, which we illustrate here with an example. To reduce the symbol $\{0, 12/5\}$, we compute that

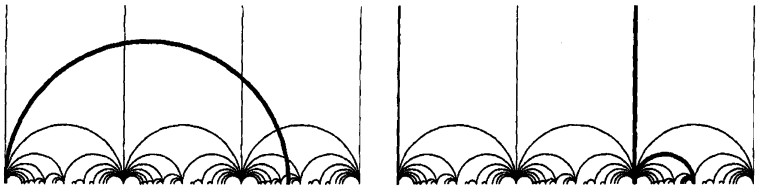
$$\frac{12}{5} = 2 + \frac{1}{2 + \frac{1}{2}}$$

has convergents $2, 5/2, 12/5$. The modular symbol reduction algorithm applied to the symbol $\{0, 12/5\}$ is

$$\{0, \frac{12}{5}\} = \{0, \infty\} + \{\infty, 2\} + \{2, \frac{5}{2}\} + \{\frac{5}{2}, \frac{12}{5}\}.$$

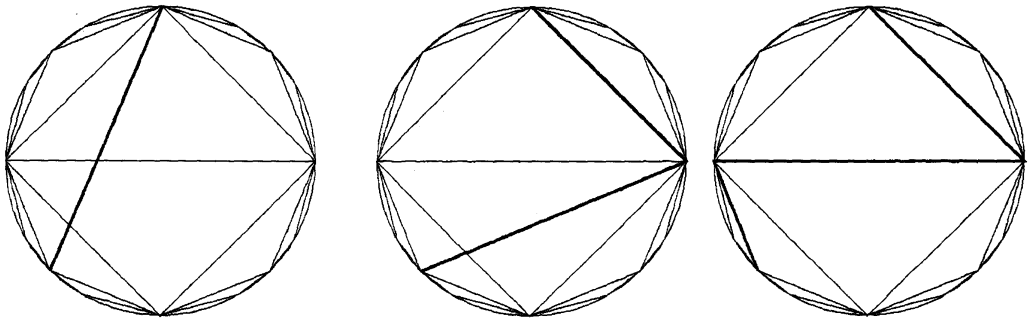
We can think of a modular symbol as a (sum of) directed geodesic joining the cusps. We show the modular symbol $\{0, 12/5\}$ and its reduction in Figure 3.

Since out goal is to generalize these techniques, we note that unimodular symbols correspond to edges of Π. Thus the problem of reducing a modular symbol can be viewed as finding a path along edges of Π, joining the two cusps. We can achieve such a reduction using an iterative process making the symbol more and more reduced. Specifically, one can "measure" how bad a symbol is by counting the number of cones for which the segment intersects the interior of the cone. For example, in Figure 4, we see that $\{0, 12/5\}$ goes through 3 cones. After one step, it is replaced by a sum of symbols, of which one goes through 2 cones, and the other goes through none. Finally, we have 3 segments, none of which intersect the interiors of the cones. This measure of "badness" is related to the determinant of a modular symbol.



Non-reduced modular symbol. Fully reduced.

FIGURE 3. The modular symbol $\{0, 12/5\}$ and its reduction in $\mathfrak{h}$.



Non-reduced modular symbol. More reduced. Fully reduced.

FIGURE 4. The modular symbol $\{0, 12/5\}$ and its reduction in C.

3. Generalizations and difficulties

In this section, we discuss generalizations of the objects introduced above, and explain some of the difficulties and subtleties that arise.

3.1. **Background.** Let F be a number field, and let $\mathcal{O} \subset F$ denote its ring of integers. Let $\mathbf{G}$ be the algebraic group $\mathbf{G} = \mathrm{Res}_{F/\mathbb{Q}} \mathrm{GL}_n$. The group of real points

$$G = \mathbf{G}(\mathbb{R}) \simeq \prod \mathrm{GL}_n(F_v), \tag{1}$$

where the product is taken over the infinite places of F, with one place taken for each complex conjugate pair.

A subgroup Γ of of $\mathbf{G}(\mathbb{Q})$ is called an *arithmetic subgroup* if it is commensurable with the group of integer points $\mathbf{G}(\mathbb{Z})$. Borel conjectured and Franke [Fra98] proved that the cohomology of arithmetic groups can be computed in terms of certain automorphic forms. The compact case is investigated in earlier work of Matsushima-Murakami [MM63]. This generalizes the Eichler-Shimura isomorphism, and these cohomology classes represent the "modular forms" that we consider.

Explicit computations in this context have been carried out in a variety of cases such as Ash-McConnell [AM92a, AM92b] for $n = 3$ and $F = \mathbb{Q}$. Ash-Gunnells-McConnell [AGM02, AGM08, AGM10] explore the case $n = 4$ with $F = \mathbb{Q}$. For $n = 2$, Cremona and his students [Cre84, CW94, Lin05, Byg98] have done computations for complex quadratic fields, Socrates–Whitehouse [SW05] and Dembélé [Dem05] for real quadratic fields. For $n = 2$ and F a totally real number field, we refer to work of Greenberg-Voight [GV09] and the references there.

3.2. **Positive definite forms.** There is a natural generalization from the space of quadratic forms and corresponding cone of positive definite forms for studying $\mathrm{GL}_2(\mathbb{Z})$ to an

analogous space of Hermitian forms and corresponding positive definite forms for studying $\mathrm{GL}_n(\mathcal{O})$. More precisely, we let $\mathrm{Sym}_n(\mathbb{R})$ denote the (real) vector space of $n \times n$ matrices with real entries, and let $\mathrm{Herm}_n(\mathbb{C})$ denote the (real) vector space of Hermitian $n \times n$ matrices with complex entries. Let

$$V = \prod V_v, \quad \text{where}$$
$$V_v = \begin{cases} \mathrm{Sym}_n(\mathbb{R}) & \text{if } v \text{ is real,} \\ \mathrm{Herm}_n(\mathbb{C}) & \text{if } v \text{ is complex.} \end{cases}$$

Note that in light of (1), we have a natural action of G on V that is analogous to the classical case. By abuse of notation, we will use the subscript of v on an object A to mean the image of A in F_v, or related structure. For example, we let $C \subset V$ denote the product $C = \prod C_v$, where $C_v \subset V_v$ is the cone of positive definite forms in V_v. As before, we can define a map $q\colon \mathcal{O}^n \to \bar{C}$ by

$$(q(x))_v = x_v x_v^*,$$

where * is complex conjugate transpose if v is complex and transpose if v is real.

Definition 3.1. The *Voronoï polyhedron* $\Pi \subset \bar{C}$ is the convex hull of

$$\{q(x) \mid x \in \mathcal{O}^n \setminus 0\}.$$

Koecher [Koe60] and Ash [Ash84] generalize Voronoï's work and show that Π has very nice structure. Though it is an infinite polyhedron, there are only finitely many facets modulo the action of $\mathrm{GL}_n(\mathcal{O})$, and the facets are in bijection with $\mathrm{GL}_n(\mathcal{O})$-classes of perfect forms.

We think of a point $A \in C$ as a quadratic form $\mathcal{O}^n \to \mathbb{Q}$ by

$$A(x) = \sum_v x_v^* A_v x_v.$$

With this interpretation we have notions of minimal vectors and perfection.

Definition 3.2. Let $A \in C$. The *minimum* of A is

$$m(A) = \min_{x \in \mathcal{O}^n \setminus \{0\}} (A(x)).$$

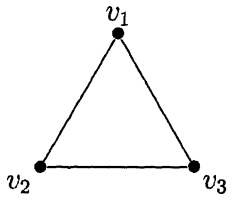
A vector $x \in \mathcal{O}^n \setminus \{0\}$ is a *minimal vector* of A if $A(x) = m(A)$. The collection of minimal vectors of A is denoted $M(A)$. A form is *perfect* if it is uniquely determined by $m(A)$ and $M(A)$.

Since the facets of Π correspond to perfect forms, one can use techniques from Voronoï theory to compute the structure of the polyhedron. We refer the reader to [Gun99, Yas09a] and references there for details.

3.3. **Sharbly complex.** The *sharbly complex* [LS76] is a homology complex with modular symbols in degree 0.

Definition 3.3. Let S_k, $k \geq 0$, be the Γ-module A_k/C_k, where A_k is the set of formal $\mathbb{C}$-linear sums of symbols $[v] = [v_1, \cdots, v_{k+n}]$, where each v_i is in F^n, and C_k is the submodule generated by

1. $[v_{\sigma(1)}, \cdots, v_{\sigma(k+n)}] - \mathrm{sgn}(\sigma)[v_1, \cdots, v_{k+n}]$,
2. $[v, v_2, \cdots, v_{k+n}] - [w, v_2, \cdots v_{k+n}]$ if $Ray(vv^*) = Ray(ww^*)$, and
3. $[\mathbf{v}]$, if $\mathbf{v}$ is *degenerate*, i.e., if $v_1, \cdots, v_{k+n}$ are contained in a hyperplane,



with the usual boundary map

$$\partial([v_1, v_2, \cdots, v_m]) = \sum_i (-1)^i [v_1, v_2, \cdots, \hat{v_i}, \cdots, v_m]$$

The boundary map commutes with the action of Γ. The *sharbly complex* $S_*(\Gamma)$ is the homological complex of coinvariants. Specifically, $S_k(\Gamma)$ is the quotient of S_k by relations of the form $\gamma \cdot \mathbf{v} - \mathbf{v}$, where $\gamma \in \Gamma$ and $\mathbf{v} \in S_k$.

Work of Borel-Serre and Ash show that the cohomology of the arithmetic group $\Gamma \subset \mathrm{GL}_n(\mathcal{O})$ can be computed in terms of the sharbly complex:

Theorem 3.4 ([BS73, Ash94]). *We have*

$$H^{\nu-k}(\Gamma; \mathbb{C}) \simeq H_k(S_*(\Gamma)), \quad \textit{where } \nu = \mathrm{vcd}(\Gamma).$$

From this point of view, we want to look as close to top-degree as possible since the relevant cohomology space corresponds to low degree homology groups. However, the cuspidal space is known to vanish outside of a strip centered about middle dimension [LS04]. In our cases of interest, the virtual cohomological dimension is $n-1$ less than the dimension of the associated symmetric space.

We examine a few examples when $n = 2$. For the classical case, the dimension of $\mathfrak{h}$ is 2, and so the cusp forms occur in a strip centered about 1. The cohomological dimension is $\nu = 1$, and so cusp forms can be computed in terms of $H^1(\Gamma; \mathbb{C}) \simeq H_0(S_*(\Gamma))$. Analogously, when F is a complex quadratic field, the symmetric space is the hyperbolic 3-plane, and we can "see" cusp forms in $H_0(S_*(\Gamma))$. For F a real quadratic field, the cusp forms do not occur in the cohomological dimension, and so we must compute in $H_1(S_*(\Gamma))$. A similar phenomena occurs for F a CM-quartic field. In this latter case, we are computing the cusp forms corresponding to classes in $H^6(\Gamma; \mathbb{C})$ by computing $H_1(S_*(\Gamma))$.

When computing in $H_k(S_*(\Gamma))$, we use k-sharblies. We see that modular symbols correspond to 0-sharblies. In this context, unimodular symbols are replaced with *Voronoï-reduced 0-sharblies*, which correspond to edges of the Voronoï polyhedron. The general reduction algorithm is described in [Gun99]. It is implemented by the author in MAGMA [BCP97, Yas09b] for Bianchi cusp forms ($n = 2$, F complex quadratic).

We can generalize these notions to define *Voronoï-reduced k-sharblies* to be those which correspond to $(k+1)$-faces of the Voronoï polyhedron.

Generalizing the techniques introduced in [Gun00], we develop a reduction algorithm for 1-sharblies in [GY08, GHY11] when $n = 2$ and F a real quadratic or CM-quartic field, which we describe below.

We think of a 1-sharbly $\mathbf{v}$ as a triangle, with vertices labeled by the spanning vectors of $\mathbf{v}$. The boundary 0-sharblies correspond to the edges of the triangle.

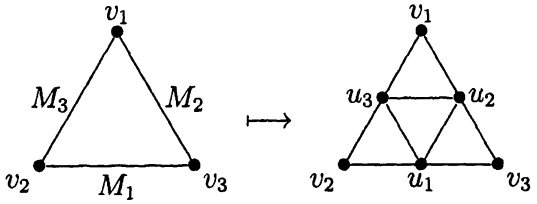
A 1-sharbly chain $\xi = \sum a(\mathbf{v})\mathbf{v}$ can be thought of a collection of triangles with vertices labeled by rays in $\bar{C}$. If ξ becomes a cycle in $S_1(\Gamma)$, then its boundary must vanish modulo

Γ. To ensure that cycles get sent to cycles, any choices made at each stage of the reduction process must be made Γ-equivariantly. This can be achieved by including a bit of extra data in the form of a *lift matrix* for each edge.

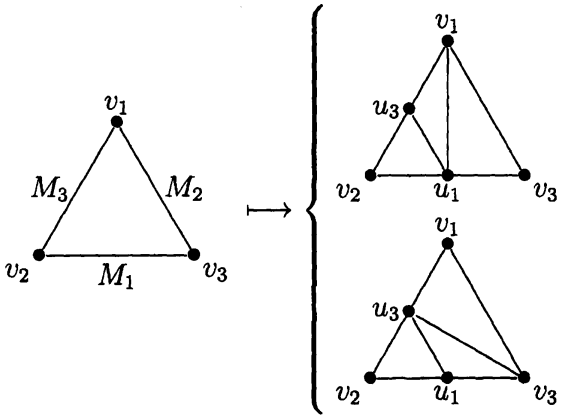
Let T be a non-degenerate 1-sharbly. The method of subdividing depends on the number of edges of T that are Voronoï reduced. The reduction algorithm can be viewed as a two stage process.

1. If T is "far" from being Voronoï reduced, one tries to replace T by a sum of 1-sharblies that are more reduced in that the edges have smaller size.
2. If T is "close" to being Voronoï reduced, then one must use the geometry of the Voronoï cones more heavily.

This process requires the computation of a *reducing point* for each non-reduced 0-sharbly in the boundary of the non-reduced 1-sharbly as well as a final refinement of choosing reducing points for 1-sharblies whose boundary 0-sharblies are reduced. The latter subtlety arises because of the infinite units in $\mathcal{O}$. Rather than give the details that go into deciding which reduction type to use at each stage, we refer the reader to [GY08, GHY11], and just give the schematics of the types of reductions that are used.

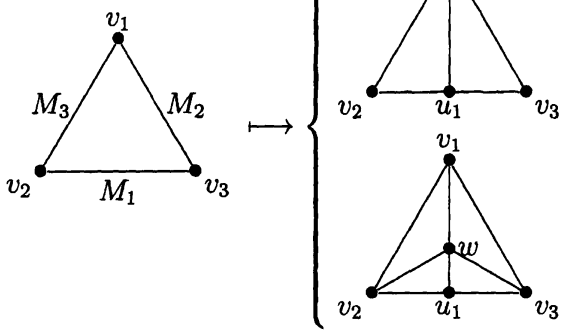


if Type I.



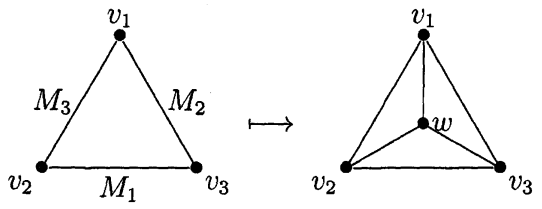
if Type II.1,

if Type II.2.



if Type III.1,

if Type III.2.



if Type IV.

4. Data for $\mathrm{GL}_2/\mathbb{Q}(\zeta_5)$

In this final section, we collect some data for the case $n = 2$ and where F is the cyclotomic field of the title. It involved a careful implementation of the theoretical considerations described above. Let F be the cyclotomic field $F = \mathbb{Q}(\zeta)$, where ζ is a primitive fifth root of unity. Let $\mathcal{O} \subset F$ denote the ring of integers of F. Let $\mathfrak{n} \subset \mathcal{O}$ be an ideal, and let $\Gamma_0(\mathfrak{n}) \subset \mathrm{GL}_2(\mathcal{O})$ be the congruence group

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathcal{O}) \;\middle|\; c \in \mathfrak{n} \right\}.$$

We remark that in the cohomology computations, following a standard practice (cf. [AGM02]) we did not work over the complex numbers $\mathbb{C}$, but instead computed cohomology with coefficients in the large finite field $\mathbb{F}_{12379}$. This technique was used to avoid the precision problems in floating-point arithmetic. We expect that the Betti numbers we report coincide with those one would compute for the group cohomology with $\mathbb{C}$-coefficients.

We were able to motivically account for every rational Hecke eigenclass we computed. All eigenclasses that appeared to come from classes over $\mathbb{Q}$ and $F^+ = \mathbb{Q}(\sqrt{5})$ were found using tables computed by Cremona [Cre06] and tables/software due to Dembélé [Dem05]. For each of the rational eigenclasses that do not come from $\mathbb{Q}$ and F^+, for all but one our searches found elliptic curves over $\mathbb{Q}(\zeta_5)$ whose point counts matched the eigenvalue data. This includes one elliptic curve of norm conductor 3641 found by Watkins after conducted a successful targeted search for the missing curve by modifying techniques of Cremona-Lingham [CL07].

Conversely, within the range of our computations we were able to cohomologically account for all the elliptic curves over F that we found. That is, we found no elliptic curve over F that was not predicted by a rational Hecke eigenclass.

4.1. **Voronoï data.** We begin with a description of the Voronoï polyhedron Π for binary Hermitian forms over F. Details can be found in [Yas09a]. In this case, there are two non-conjugate embeddings of F to $\mathbb{C}$. Thus the space of forms V is 8-dimensional

$$V = \mathrm{Herm}_2(\mathbb{C}) \times \mathrm{Herm}_2(\mathbb{C}).$$

It follows that the corresponding symmetric space is

$$X = C/\mathbb{R}_{>0} \simeq \mathfrak{h}_3 \times \mathfrak{h}_3 \times \mathbb{R},$$

where $\mathfrak{h}_3$ is hyperbolic 3-space.

Up to the action of $\mathrm{GL}_2(\mathcal{O})$, there is exactly one perfect binary form ϕ. The associated Hermitian matrix is

$$A = \frac{1}{5}\begin{bmatrix} \zeta^3+\zeta^2+3 & \zeta^3-\zeta^2+\zeta-1 \\ -2\zeta^3-\zeta-2 & \zeta^3+\zeta^2+3 \end{bmatrix}.$$

We compute that ϕ has 240 minimal vectors. Since minimal vectors that differ by torsion units give rise to the same point in C, the corresponding facet of Π is 7-dimensional

polytope with 24 vertices. We compute that this polytope has 118 faces (14 with 12 vertices, 80 with 9 vertices, 24 with 7 vertices).

By computing the full structure of the polytope as well as the stabilizers of each of the faces, we can compute the cohomology and the action of the Hecke operators.

4.2. **Cuspidal spaces.** Details of the cohomology computations as well as the data tables can be found in [GHY11].

Our first task was to identify those levels with nonzero cuspidal cohomology. We first experimentally determined the dimensions of the subspace H^5 is spanned by Eisenstein cohomology classes. Such classes are closely related to Eisenstein series. In particular the eigenvalue of $T_\mathfrak{q}$ on these classes equals $\mathrm{N}(\mathfrak{q}) + 1$. We expect that for a given level $\mathfrak{n}$, the dimension of the Eisenstein cohomology space depends only on the factorization type of $\mathfrak{n}$. Thus initially we used some Hecke operators applied to cohomology spaces of small level norm to compute the expected Eisenstein dimension for small levels with different factorization types.

We then computed cohomology for a larger range of levels and looked for Betti numbers in excess of that predicted value. We were able to compute H^5 for all levels $\mathfrak{n}$ with $\mathrm{N}(\mathfrak{n}) \leq 4941$. For $\mathfrak{n}$ prime we were able to carry the computations further to $\mathrm{N}(\mathfrak{n}) \leq 7921$. It turns out that in the range of our computation, modulo the action of Galois each cuspidal space can be uniquely identified by the norm of the level, except when $\mathrm{N}(\mathfrak{n}) = 3641$. In this case there are two levels up to Galois conjugacy with nonzero cuspidal cohomology; we call them 3641a and 3641b.

Next we computed the Hecke operators and looked for eigenclasses with rational eigenvalues. These computations were quite intensive. For all levels we were able to compute at least up to $T_\mathfrak{q}$ with $\mathfrak{q} \subset \mathcal{O}$ prime satisfying $\mathrm{N}(\mathfrak{q}) \leq 41$; at some smaller levels, such as $\mathrm{N}(\mathfrak{n}) = 701$, we computed much further. At the largest levels ($\mathrm{N}(\mathfrak{n}) = 4455, 4681, 6241, 7921$) the computation was so big that our implementation could not compute any Hecke operators.

For all levels except for one, the cuspidal cohomology split into 1-dimensional rational eigenspaces. The remaining cuspidal space at level of norm 3721 is 2-dimensional with Hecke eigenvalues generating the field $F^+ = \mathbb{Q}(\sqrt{5})$.

4.3. **Elliptic curves over F.** Now we give motivic explanations for all the cuspidal cohomology we found. Thirteen of the eigenclasses have the property that their eigenvalues $a_\mathfrak{q}$ differ for at least two primes $\mathfrak{q}$, $\mathfrak{q}$ lying over the same prime in the subfield F^+ . Hence we expect these classes to correspond to elliptic curves over F. We were able to find elliptic curves E/F such that for all primes $\mathfrak{q}$ of good reduction, the identity $a_\mathfrak{q} = \mathrm{N}(\mathfrak{q}) + 1 - |E(\mathbb{F}_\mathfrak{q})|$ held for every Hecke operator we computed.

4.4. **The remaining eigenclasses.** All the other eigenclasses in can be accounted for either by elliptic curves over $\mathbb{Q}$, elliptic curves over F^+, "old" cohomology classes coming from lower levels, or other Hilbert modular forms over F^+. We indicate briefly what happens.

4.4.1. *Elliptic curves over* $\mathbb{Q}$. The eigenclasses at 400, 405, 1280, 1296, 4096, and one of the eigenclasses at 2025, correspond to elliptic curves over $\mathbb{Q}$ that can readily be found in Cremona's tables [Cre06]. In all cases, there are actually two rational elliptic curves that are not isogenous over $\mathbb{Q}$ but produce the same eigenvalue data when considered as curves over F; the curves in these pairs are quadratic twists by 5 of each other that

become isomorphic over F^+. For instance, at 400 the two curves are 50A1 and 50B3 in the notation of [Cre06].

4.4.2. *Elliptic curves over F^+.* The eigenclasses at 605, 961, 1681, 1805, 2401, and 4205 correspond to elliptic curves over F^+. The class at 2401 already appears in [Dem05]; the others were verified using software written by Dembélé. As an example, the three eigenclasses at 4205 correspond to three cuspidal parallel weight 2 Hilbert modular newforms of level $\mathfrak{p}_5\mathfrak{p}_{29} \subset \mathcal{O}_{F^+}$. Although we were unable to compute Hecke operators at 6241 and 7921, we expect that these classes correspond to elliptic curves given in [Dem05].

4.4.3. *Old classes.* There are 2-dimensional eigenspaces at 2000, 2025, 3025, 3505, 4400, and 4455 on which the Hecke operators we computed act by scalars. These subspaces correspond to curves appearing at lower levels. For example, the classes at 2000 and 4400 correspond to the classes that already appeared at 400. We note that 2000, 2025, 4400, and 4455 correspond to elliptic curves over $\mathbb{Q}$, while 3025 corresponds to an elliptic curve over F^+ seen at norm conductor 605 and 3505 to a curve over F seen at norm conductor 701.

4.4.4. *Other Hilbert modular forms.* There are two eigenclasses remaining, namely the class at 3721 with eigenvalues in F^+ and the third eigenclass ξ at 3025 with eigenvalues in $\mathbb{Q}$. Both can be attributed to Hilbert modular forms of parallel weight 2 attached to abelian surfaces.

For 3721, the characteristic polynomials match those of a parallel weight 2 Hilbert modular newform of level $\mathfrak{p}_{61} \subset \mathcal{O}_{F^+}$. For dimension reasons, one can actually prove that this form is the base change from F^+ of a Hilbert modular form corresponding to an abelian surface with real multiplication by the ring of algebraic integers in $\mathbb{Q}(\sqrt{5})$ The abelian surface in question is discussed in Dembélé-Voight [DV].

The class ξ at 3025 is perhaps the most interesting of all, other than the classes matching elliptic curves over F. Let $\mathfrak{m} \subset \mathcal{O}_{F^+}$ be the ideal $\mathfrak{p}_{25}\mathfrak{p}_{11}$. The space of parallel weight 2 Hilbert modular newforms of level m contains an eigenform g with Hecke eigenvalues $a_\mathfrak{q}$ in the field F^+. For any prime $\mathfrak{q} \subset \mathcal{O}_{F^+}$, let $q \in \mathbb{Z}$ be the prime under $\mathfrak{q}$. Then we have $a_\cdot('g) = 0$ if $q = 5$,and

$$a_\mathfrak{q}(g) \in \begin{cases} \mathbb{Z} & \text{if } q = 1 \mod 5, \\ \mathbb{Z} \cdot \sqrt{5} & \text{if } q = 2, 3, 4 \mod 5. \end{cases} \tag{2}$$

The conditions (2) imply that the L-series $L(s, g)L(s, g \otimes \epsilon)$ agrees with the L-series attached to our eigenclass ξ, where ϵ is the unique quadratic character of $\mathrm{Gal}(F/F^+)$. Indeed, following [Cre92], if $\mathfrak{q} \subset \mathcal{O}_{F^+}$ splits in F as $\mathfrak{r} \cdot \bar{\mathfrak{r}}$ (respectively, remains inert in F), then we should expect the Hecke eigenvalues of g and ξ to be related by

$$a_\mathfrak{r}(\xi) = a_{\bar{\mathfrak{r}}}(\xi) = a_\mathfrak{q}(g) \quad \text{(split)}$$

and

$$a_\mathfrak{q}(\xi) = a_\mathfrak{q}(g)^2 - 2\,\mathrm{N}_{F^+/\mathbb{Q}}(\mathfrak{q}) \quad \text{(inert)}.$$

From the "modular/automorphic" viewpoint, these forms are, on the one hand, simply a result of base change from F^+ to F, and on the other hand, a striking example of an intriguing phenomenon. From this point of view, with $\mathfrak{m} = \mathfrak{p}_{25}\mathfrak{p}_{11} \subset \mathcal{O}_{F^+}$, the dimension of the new subspace of Hilbert modular forms of level $\mathfrak{m}$ and parallel weight 2 is

$$\dim S_2(\mathfrak{m})^{\text{new}} = 3 = 1 + 2.$$

There is a Shimura curve $X_0^B(\mathfrak{m})$ attached to (an Eichler order of level $\mathfrak{m}$ in) the quaternion algebra ramified only at one infinite place and $\mathfrak{p}_{11}$. The new part of its Jacobian satisfies

$$J_0^B(\mathfrak{m})^{\text{new}} = E_f \times A_g,$$

where E_f is an elliptic curve and A_g is an abelian surface with real multiplication by $\mathbb{Q}(\sqrt{5})$. The surface A_g splits into two elliptic curves over F. One can also see the elliptic curve E_f at norm 3025 as an old form as previously described.

References

[AGM02] Avner Ash, Paul E. Gunnells, and Mark McConnell, *Cohomology of congruence subgroups of* $\mathrm{SL}_4(\mathbb{Z})$, J. Number Theory **94** (2002), no. 1, 181–212. MR 1904968 (2003f:11072)

[AGM08] ———, *Cohomology of congruence subgroups of* $\mathrm{SL}(4,\mathbb{Z})$. *II*, J. Number Theory **128** (2008), no. 8, 2263–2274. MR 2394820 (2009d:11084)

[AGM10] ———, *Cohomology of congruence subgroups of* $\mathrm{SL}_4(\mathbb{Z})$. *III*, Math. Comp. **79** (2010), no. 271, 1811–1831. MR 2630015 (2011e:11095)

[AM92a] Avner Ash and Mark McConnell, *Doubly cuspidal cohomology for principal congruence subgroups of* $\mathrm{GL}(3,\mathbf{Z})$, Math. Comp. **59** (1992), no. 200, 673–688. MR MR1134711 (93b:11066)

[AM92b] ———, *Experimental indications of three-dimensional Galois representations from the cohomology of* $\mathrm{SL}(3,\mathbf{Z})$, Experiment. Math. **1** (1992), no. 3, 209–223. MR MR1203875 (94b:11045)

[Ash84] Avner Ash, *Small-dimensional classifying spaces for arithmetic subgroups of general linear groups*, Duke Math. J. **51** (1984), no. 2, 459–468. MR MR747876 (85k:22027)

[Ash94] ———, *Unstable cohomology of* $\mathrm{SL}(n,\mathcal{O})$, J. Algebra **167** (1994), no. 2, 330–342. MR 1283290 (95g:20050)

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic). MR MR1839918 (2002d:11058)

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478

[BS73] A. Borel and J.-P. Serre, *Corners and arithmetic groups*, Comment. Math. Helv. **48** (1973), 436–491, Avec un appendice: Arrondissement des variétés à coins, par A. Douady et L. Hérault. MR MR0387495 (52 #8337)

[Byg98] J. Bygott, *Modular forms and modular symbols over imaginary quadratic fields*, Ph.D. thesis, Exeter University, 1998.

[CDT99] Brian Conrad, Fred Diamond, and Richard Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), no. 2, 521–567. MR MR1639612 (99i:11037)

[CL07] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. **16** (2007), no. 3, 303–312. MR 2367320 (2008k:11057)

[Cre84] J. E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Math. **51** (1984), no. 3, 275–324. MR MR743014 (85j:11063)

[Cre92] ———, *Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields*, J. London Math. Soc. (2) **45** (1992), no. 3, 404–416. MR 1180252 (93h:11056)

[Cre06] John Cremona, *The elliptic curve database for conductors to 130000*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 11–29. MR 2282912 (2007k:11087)

[CW94] J. E. Cremona and E. Whitley, *Periods of cusp forms and elliptic curves over imaginary quadratic fields*, Math. Comp. **62** (1994), no. 205, 407–429. MR MR1185241 (94c:11046)

[Dem05] Lassina Dembélé, *Explicit computations of Hilbert modular forms on* $\mathbb{Q}(\sqrt{5})$, Experiment. Math. **14** (2005), no. 4, 457–466. MR MR2193808 (2006h:11050)

[Dia96] Fred Diamond, *On deformation rings and Hecke rings*, Ann. of Math. (2) **144** (1996), no. 1, 137–166. MR MR1405946 (97d:11172)

[DV] Lassina Dembélé and John Voight, *Explicit methods for hilbert modular forms*, submitted.

[Fra98] Jens Franke, *Harmonic analysis in weighted L_2-spaces*, Ann. Sci. École Norm. Sup. (4) **31** (1998), no. 2, 181–279. MR MR1603257 (2000f:11065)

[GHY11] Paul E. Gunnells, Farshid Hajir, and Dan Yasaki, *Modular forms and elliptic curves over the field of fifth roots of unity*, Experimental Mathematics (2011), accepted.

[Gun99] Paul E. Gunnells, *Modular symbols for $\mathbf{Q}$-rank one groups and Voronoĭ reduction*, J. Number Theory **75** (1999), no. 2, 198–219. MR MR1681629 (2000c:11084)

[Gun00] ———, *Computing Hecke eigenvalues below the cohomological dimension*, Experiment. Math. **9** (2000), no. 3, 351–367. MR MR1795307 (2001k:11092)

[GV09] Matthew Greenberg and John Voight, *Computing systems of Hecke eigenvalues associated to Hilbert modular forms*, 1–20, `arXiv:0904.3908`.

[GY08] Paul E. Gunnells and Dan Yasaki, *Hecke operators and Hilbert modular forms*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 387–401. MR MR2467860

[Hab83] Klaus Haberland, *Perioden von Modulformen einer Variabler and Gruppencohomologie. I, II, III*, Math. Nachr. **112** (1983), 245–282, 283–295, 297–315. MR 726861 (85k:11022)

[Koe60] Max Koecher, *Beiträge zu einer Reduktionstheorie in Positivitätsbereichen. I*, Math. Ann. **141** (1960), 384–432. MR MR0124527 (23 #A1839)

[Lin05] Mark Lingham, *Modular forms and elliptic curves over imaginary quadratic fields*, Ph.D. thesis, University of Nottingham, 2005.

[LS76] Ronnie Lee and R. H. Szczarba, *On the homology and cohomology of congruence subgroups*, Invent. Math. **33** (1976), no. 1, 15–53. MR MR0422498 (54 #10485)

[LS04] Jian-Shu Li and Joachim Schwermer, *On the Eisenstein cohomology of arithmetic groups*, Duke Math. J. **123** (2004), no. 1, 141–169. MR MR2060025 (2005h:11108)

[MM63] Yozô Matsushima and Shingo Murakami, *On vector bundle valued harmonic forms and automorphic forms on symmetric riemannian manifolds*, Ann. of Math. (2) **78** (1963), 365–416. MR 0153028 (27 #2997)

[SW05] Jude Socrates and David Whitehouse, *Unramified Hilbert modular forms, with examples relating to elliptic curves*, Pacific J. Math. **219** (2005), no. 2, 333–364. MR 2175121 (2007c:11059)

[TW95] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572. MR MR1333036 (96d:11072)

[Vor08] G. Voronoĭ, *Sur quelques propriétés des formes quadratiques positives parfaites*, J. Reine Angew. Math. **133** (1908), 97–178.

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR MR1333035 (96d:11071)

[Yas09a] Dan Yasaki, *Binary Hermitian forms over a cyclotomic field*, J. Algebra **322** (2009), 4132–4142.

[Yas09b] ———, *Modular forms over imaginary quadratic fields*, MAGMA V2.16, 2009.

DEPARTMENT OF MATHEMATICS AND STATISTICS, THE UNIVERSITY OF NORTH CAROLINA AT GREENSBORO, GREENSBORO, NC 27402-6170, USA

E-mail address: `d_yasaki@uncg.edu`